



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/695,837	10/30/2003	Tzahi Carmeli	P-5763-US	7206
49444	7590	10/04/2007	EXAMINER	
PEARL COHEN ZEDEK LATZER, LLP 1500 BROADWAY, 12TH FLOOR NEW YORK, NY 10036			LEMMA, SAMSON B	
ART UNIT		PAPER NUMBER		
2132				
MAIL DATE		DELIVERY MODE		
10/04/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	10/695,837	CARMELI, TZAHI
	Examiner	Art Unit
	Samson B. Lemma	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 12 September 2007.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1,2,4-19 and 26-36 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1,2, 4-19 and 26-36 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____	6) <input type="checkbox"/> Other: _____

***DETAILED ACTION***

1. The request filed September 12, 2007 for a request for continued examination (RCE) under 37 CFR 1.114 based on patent application 10/695,837 is acceptable and an RCE has been established. Every Independent **claims 1, 12, 26 and 32** has been amended. Claims 3 and 20-25 have been canceled. No new claims are added. Thus **claims 1-2, 4-19 and 26-36** are pending/examined.

***Response to Arguments***

2. Applicant's remark/arguments filed on September 12, 2007 have been fully considered but are moot in view of the new ground/s of rejection.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner

4. **Claims 1-2, 4-19 and 26-36** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Callum** (Hereinafter referred as **Callum**) (U.S. Patent No. 6,295,604, Patent Date September 25, 2001) in view of **Kean** (hereinafter referred as **Kean**)(U.S. Patent No: 7,203,842) (filed on December 21, 2000).

5. **As per independent claims 1, 12, 26 and 32 Callum discloses a method comprising:**

- **Receiving a date frame comprising a header and a data portion.** *[Column 5, lines 17-2] (Packet controller 240 receives a data packet from memory controller 220, and this data packet is comprises of a header having a control information and data portion and the packet controller 240 then separates the control information in its header from the data portion)*
- **If the header indicates transmitting, configuring transmitter to encrypt the data frame** *[Column 5, lines 17-24] (Packet controller 240 separately transmits this header information across signal lines 260 and 270, respectively. Cryptographic unit 250 which is interpreted as the transmitter/receiver encrypts the contents of the data portion in accordance with the control information provided by the header, implies that if the header information indicates encryption then the cryptographic unit 250 encrypts the data and inherently transmit the encrypted data/cipher) and;*
- **If the header indicates receiving configuring a receiver to decrypt the data frame** *[Column 5, lines 17-24] (Packet controller 240 separately transmits this header information across signal lines 260 and 270, respectively. Cryptographic unit 250 which is interpreted as the transmitter/receiver decrypts the contents of the data portion in accordance with the control information*

*provided by the header, implies that if the header information indicates decryption then the cryptographic unit 250/receiver decrypts the data)*

**Callum** does not explicitly teach the feature that the header comprising one or more of the group consisting of: a frame length, an encryption key, and an initial vector;

if one or more of the frame length, the encryption key and the initial vector in the header indicates transmitting, configuring a transmitter to encrypt the data frame; and if one or more of the frame length, the encryption key, and the initial vector in the header indicates receiving, configuring a receiver to decrypt the data frame.

However, in the same field of endeavor, **Kean on at least claims 76 and 77**, discloses the above features. For instance **Kean on at least claim 76 discloses the method**, wherein the header information indicates that the security processing operation is to encrypt the unencrypted configuration information **using a key/encryption key included in the header information**, and load the encrypted configuration information into an external non-volatile memory and this meets the limitation recited as **“the header comprising one or more of the group consisting of: a frame length, an encryption key, and an initial vector; if one or more of the frame length, the encryption key and the initial vector in the header indicates transmitting, configuring a transmitter which is transmitting the data to an external non-volatile memory to encrypt the data frame”**;

**Furthermore Kean on at least claim 77 discloses the method**, wherein the header information as it is described in claim 76, includes a **key/encryption key**, indicates that the configuration information is encrypted,

and the security processing operation is to unencrypt/decrypt the encrypted configuration data and load the unencrypted configuration information into configuration memory and this meets the limitation recited as "**if one or more of the frame length, the encryption key, and the initial vector in the header indicates receiving/receiving data to be loaded into configuration memory then, configuring a receiver to decrypt the data frame.**"

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features that the header comprising an encryption key, if the encryption key in the header indicates transmitting, configuring a transmitter to encrypt the data frame; and if the encryption key, indicates receiving, configuring a receiver to decrypt the data frame as per teachings of **Kean** into the method as taught by **Callum** for the purpose providing improved techniques and circuitry for secure configuration. [See Kean on column 2, lines 41-42]

6. **As per claims 2, 13-14, 27-28 and 33-34 the combination of Callum and Kean discloses a method as applied to claims above. Furthermore, Callum discloses the method further comprising authenticating the header of the data frame and processing the header of the data frame to provide a processed header; and configuring the transmitter and the receiver based on information included in the processed header.** [See figure 3-5 and at least column 3, lines 25-column 4, line 10]
  
7. **As per claims 4-11, 15-19, 29-31 and 35-36 the combination of Callum and Kean discloses a method as applied to claims above. Furthermore, Callum discloses the method wherein configuring comprises: configuring the receiver to authenticate and decrypt a data portion and a message**

**integrity code portion of the data frame. [figure 3-5] and the method further comprising: decrypting the data portion and the message integrity code portion of the data frame to provide a decrypted data portion and a decrypted message integrity code portion, respectively; calculating the message integrity code of the data frame from the decrypted data portion; and comparing the calculated message integrity code to the decrypted message integrity code portion. [See figure 3-5 and at least column 3, lines 25-column 4, line 10] ( Referring now to FIGS. 3-5, data packet 300 includes a header 310 and a data portion 350. In this embodiment, header 310 comprises control information including a control word 320, one or more keys 330 and an initialization vector (IV) 340 as shown in FIG. 4. Control word 320 provides information to control the functionality of CPP unit 230 of FIG. 2. The keys 330 and IV 340 are used by CPP unit 230 to perform encryption or decryption operations. And As shown in FIG. 5, one embodiment of control word 320 includes a plurality of bit fields 321-324. These bit fields 321-324 provide the CPP unit with information concerning the length of data packet 300 of FIG. 3, the mode of operation (encryption/decryption), and optionally, the type of cryptographic technique used. It is contemplated that different bit lengths associated bit fields 321-324 may be utilized other than the bit lengths illustrated herein. In particular, as shown in FIGS. 3 and 5, first bit field 321 contains a byte count which indicates the number of bytes in data packet 300, and second bit field 322 includes one or more bits which indicate whether encryption or decryption is to be performed on data portion 350 of the incoming data packet. As optional bit fields of control word 320, third/forth bit fields 323 and 324 indicate the type of cryptographic operation to be performed. For example, if the CPP unit supports DES, third bit field 323 may indicate a selected DES mode (e.g., triple key DES) and fourth bit field 324 may indicate whether Cipher Block Chaining (CBC) or Electronic Codebook (ECB) is desired. The operations associated with**

CBC and ECB are set forth in a Federal Information Processing Standard Publication (FIPS Pub. 81) entitled "DES Modes of Operation" published on or around Dec. 2, 1980. It is contemplated that other types of cryptographic operations would assign bit fields 323 and 324 to provide different information. Referring back to FIGS. 2 and 4, header 310 further includes keys 330 and IV 340. In this embodiment, three (3) keys are provided, each key being at least 56-bits in length, although any bit size may be used so long as it is in accordance to the cryptographic standard followed by CPP unit 230. In the event that a 32-bit data bus is implemented between memory controller 220 and CPP unit 230, two data transfers maybe employed, in this embodiment to transfer one of the keys 330 as shown in FIG. 4. Initialization vector (IV) 340 is a binary vector used as a randomizing block of data that is exclusively OR'ed (XOR) with a first data block in CBC mode. Finally the following has been disclosed, "Referring back to FIG. 3, data portion 350 includes N data blocks 360.sub.1 -360.sub.N, where "N" is a positive whole number. In this embodiment, a "block" is a 32-bit word. The sizing of the word is constrained by the bit width of the cryptographic bus situated between memory controller 220 and CPP unit 230 of FIG. 2.")

## **Conclusion**

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See also PTO-Form 892).
  - a. US Publication No. 2005/0021961 to Hanks et al, discloses a content request is transmitted to a content provider. In response to the content request, a session key is received and **programmable hardware is configured using the session key to produce a first configuration. An identification key is generated and the first configuration of the programmable hardware is used to encrypt the identification key.** [See at least the Abstract]

Art Unit: 2132

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

**SAMSON LEMMA**

*S.L.*  
09/23/2007

*Gilberto J.*  
GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100